BRADLEY/GROMBACHER, LLP
Kiley Grombacher, Esq. (SBN 245960)
31365 Oak Crest Drive, Suite 240
Westlake Village, CA 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
Email: kgrombacher@bradleygrombacher.com

Attorneys for Plaintiff DANIEL POMEROY, on behalf of himself and others similarly situated

IN THE UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

DANIEL POMEROY, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

TICKETMASTER, LLC,

Defendant.

CASE NO.:

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE**
2. **NEGLIGENCE *PER SE***
3. **UNJUST ENRICHMENT**
4. **BREACH OF IMPLIED CONTRACT**

JURY TRIAL DEMANDED

Plaintiff Daniel Pomeroy ("Plaintiff") brings this Class Action Complaint ("Complaint") against Ticketmaster, LLC and Live Nation Entertainment, Incorporated ("Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows

I. SUMMARY OF ACTION

1. Plaintiff bring this class action against Defendant for its failure to properly secure and safeguard the personally identifiable information (PII) of its customers, including, but not limited to: full names, addresses, email addresses, phone numbers and credit card details.

2. Ticketmaster, LLC ("Ticketmaster") is one of the largest ticket sales and distribution companies in the world. Ticketmaster operates a digital ticketing platform that requires customers to provide their PII prior to purchase. Defendant revealed in a June 28, 2024 notification to the Maine Attorney General that a hacker gained unauthorized access to Defendant's cloud database, owned and operated by Snowflake, Inc., information on April 2, 2024 (the "Data Breach" or "Breach").

3. Defendant did not discover the Data Breach until May 23, 2024, nearly seven weeks later, and did not notify Plaintiff or Class Members until July 17, 2024, another almost two months after the Data Breach was discovered.

4. Plaintiff's and Class Members' personal information— which they entrusted to Defendant on the mutual understanding that Defendant would protect it against unauthorized disclosure—was compromised in a data breach (hereafter referred to as, the "Data Breach").[1]

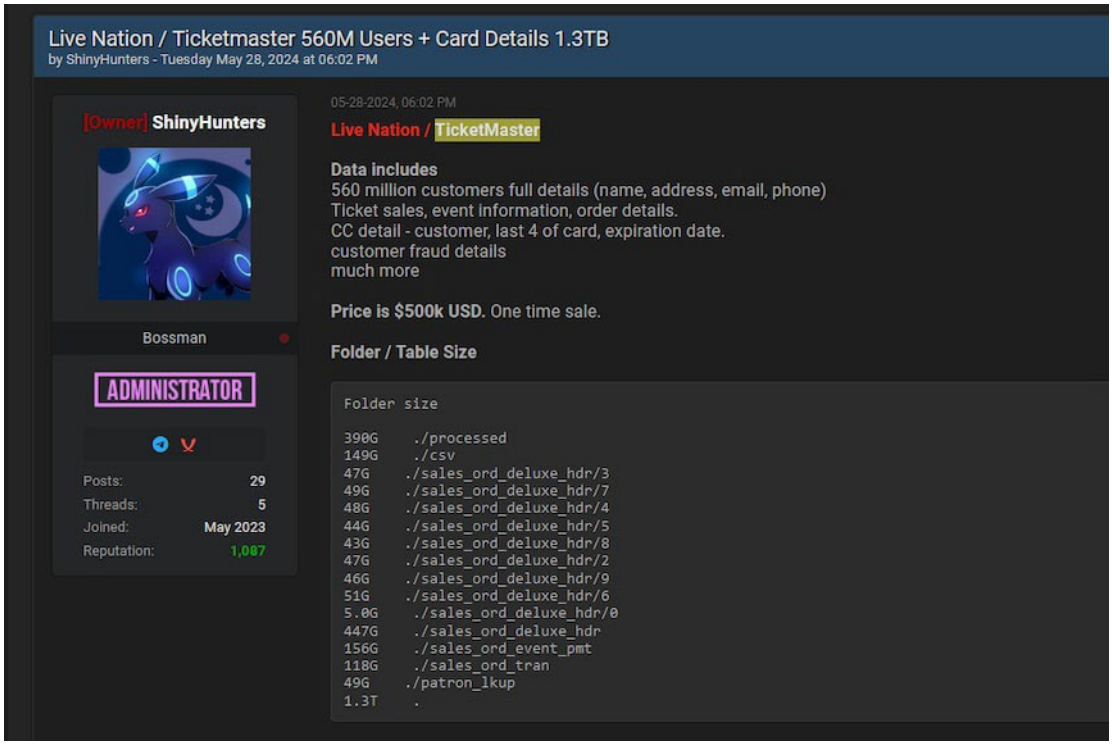
5. The Data Breach included personal details, including names, contact

[1] *Live Nation Entertainment Form 8-K,* https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm (accessed Oct. 10, 2024).

information, and payment card information, of about 560 million Ticketmaster customers.[2] The PII compromised in the Data Breach was exfiltrated by cyber-criminals who target PII for its value to identity thieves.

6. ShinyHunters, the group claiming responsibility for the Data Breach, has been linked to a string of high-profile data breaches resulting in millions of dollars in losses.[3]

7. The hackers are demanding a ransom payment of $500,000.00 to prevent the data from being resold on the dark web; a clear indication that the data breach was for the purpose of using the Plaintiff's and Class Members' personal information to perpetuate identity theft and other fraud.[4]



**Screenshot of ShinyHunters advertising the sale of Ticketmaster customer PII on the dark web.*

---

[2] *Data allegedly stolen from 560 million Ticketmaster users*, https://www.bbc.com/news/articles/c899pz84d8zo (accessed Oct. 10, 2024).

[3] *Id.*

[4] *Id.*

8. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an injury in fact. Additionally, the Plaintiff and Class Members are at an increased risk of future harm, including identity theft, fraud, spam, phishing, or other impersonation attacks.

9. There is a substantial risk of future identity theft or fraud where the Plaintiff's and Class Members' PII was targeted by a sophisticated hacker group (ShinyHunters), known for stealing and reselling as much personal and financial data as they can.[5] Furthermore, since 2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (e.g., GitHub, AT&T, Pizza Hut). Upon information and belief, ShinyHunters has accumulated enough personal information from that series of data breaches to be able to open a bank account or commit other fraud using stolen identities.

10. Plaintiff and Class Members face a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a hacker group (ShinyHunters), known for stealing and reselling personal data. For example, once a cybercriminal has sold a stolen email address or phone number, that email address or phone number is sent spam messages that are "carefully calculated to get the recipient to click on a link that infects a computer with malware."[5] Once the computer is infected with malware, the computer is locked down and the user is sent a ransom demand, which must be paid to regain access to the computer.

11. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of

---

[5] *What we know about the 'remarkably devious' ShinyHunters hackers allegedly behind the Ticketmaster data leak*, https://www.abc.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928 (accessed Oct. 10, 2024)

benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fail to implement appropriate and reasonable measures to protect the PII.

12. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable data protection procedures, including vendor management, necessary to protect consumers' PII from a foreseeable and preventable risk of unauthorized disclosure.

13. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

14. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems, or the data systems of its vendors, were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach. Plaintiff and Class Members are now at risk because of Defendant's wrongful conduct.

15. Armed with the PII acquired in the Data Breach, data thieves have already engaged in identity theft and fraud and can, in the future, commit a variety of crimes including, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information,

obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiff and Class Members may also incur out of pocket costs, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft. Plaintiff and Class Members may also incur out of pocket costs, for purchasing products to protect themselves from spam emails, phone calls, and text messages.

17. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been disclosed to an unauthorized third party and precisely what information was accessed.

18. Through this Complaint, Plaintiff seek to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff and Class Members have a continuing interest in ensuring that their personal information is kept confidential and protected from disclosure, and they should be entitled to injunctive and other equitable relief.

II. JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs, is a citizen of a state different from Defendants.

20. This Court has personal jurisdiction over Defendant because their principal place of business is in this District. Defendant have also purposefully availed

themselves of the laws, rights, and benefits of the State of California.

21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant maintain their principal place of business in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

III. PARTIES

22. Plaintiff Daniel Pomeroy is a citizen of the State of Florida. At all relevant times, Plaintiff has been a resident of Pensacola, Florida.

23. Defendant is a Virginia limited liability company with its principal place of business in Beverly Hills, California. Ticketmaster operates as a ticket distribution company; it buys, transfers, and sells tickets for live music, sporting, arts, theater, and family events around the around the world.

IV. FACTUAL ALLEGATIONS

24. Defendant promotes, operates, and manages entertainment venues and ticket sales for live entertainment events. Defendant permit users to buy and sell tickets online for concerts, sports, theater, family, and other events using the website www.ticketmaster.com.

25. Plaintiff and Class Members are current and former customers of Ticketmaster and have used, or created accounts on, ticketmaster.com.

26. In the course of their relationship, customers, including Plaintiff and Class Members, provided Defendant with at least the following: full names, dates of birth, contact information, and credit card, debit card, or banking information.

27. Upon information and belief, while collecting PII from customers, including Plaintiffs, Defendant promised to provide security measures to protect customer information. When customer data is transferred to a third-party, Defendant promised to "ensure that appropriate safeguards are put in place" to ensure customer data is "protected to the highest standard."[6] More specifically, when personal

[6] *Ticketmaster Privacy Policy*, https://privacy.ticketmaster.com/privacy-policy (accessed June 11, 2024).

information is transferred to a third party, Defendant represented that they would "use contractual measures and internal mechanisms requiring the recipient to comply with the privacy standards of the exporter."[7] These promises were contained in the applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. Plaintiff and the Class Members, as customers of Defendants, relied on these representations and on these sophisticated business entities to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

29. On May 20, 2024, Live Nation identified unauthorized activity within a third-party cloud database environment containing personal data (primarily from its Ticketmaster L.L.C. subsidiary).[8] On May 27, 2024, Live Nation discovered that the personal details of about 560 million Ticketmaster customers—including Plaintiff and Class Members—was exfiltrated by cyber-criminals demanding a ransom payment of $500,000.00 to prevent the data from being resold on the dark web.

30. Information disclosed by ShinyHunters, the cyber-criminals responsible for the Data Breach, indicates the stolen information includes "a treasure trove of sensitive user information, including full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data."[9]

31. With the information that was accessed in the Data Breach, "cybercriminals can commit identity theft and financial fraud, launch phishing attacks,

---

[7] *Id.*

[8] *Id.*

[9] *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500K*, https://hackread.com/hackers- ticketmaster-data-breach-560m-users-sale (accessed June 11, 2024).

or take over online accounts. They may also use the data for blackmail, extortion, medical identity theft or credential stuffing which could lead to significant financial losses for customers, [and] damage to credit scores."[10]

32. Data stolen in the Data Breach included unencrypted customer data that had been shared or stored with a third-party cloud database vendor. Plaintiff further believes that his PII and that of the Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of the ShinyHunters group and other cybercriminals that commit cyber-attacks of this type.

33. Defendant collects and sell the PII of its customers, former customers, and other personnel. Defendant collects personal information when a customer buys merchandise or a ticket to an event. Defendant then sell personal information like names, physical addresses, phone numbers, email addresses, IP addresses, information about transactions, preferences, and attributes, cookies and device attributes to business partners, data brokers, and service providers.[11]

34. By obtaining, collecting, and using Plaintiff'sand Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff'sand Class Members' PII from unauthorized disclosure.

35. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendant absent a promise to safeguard that information. Indeed, Defendant makes the following representations to customers on their ticketmaster.com website:

a. "The security of our fans' information is a priority for us."

b. "We take all necessary security measures to protect personal information that's shared and stored with us."

c. "We work with our partners to put on amazing live events and

[10] *Id.*

[11] *Id.*

provide additional services that we think you'll love. We always ask them to maintain the same standards of privacy."

d. "We embed privacy in the development of our products and services to ensure that we always respect your personal information."

e. "As an international company, no matter where you are located, our control framework is built around global data protection laws."

f. "We comply with all applicable data protection laws and listen to your expectations when it comes to how your information is handled."

g. "We have a global privacy team of trust and security professionals that ensure end- to-end protection of your personal information throughout the data lifecycle."[12]

36. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to ensure that third-party vendors adhered to reasonable security measures, to use this information for business purposes only, and to permit only authorized uses and disclosures of this information.

37. Defendant's representations about their commitment to security and confidentiality of the personal information they collect and share with third parties was false or misleading as an unauthorized person was able to access and exfiltrate personal data from one of Defendant's cloud database vendors. Defendant have failed to maintain the confidentiality and security of Plaintiff'sand the Class Members' PII and/or failed to take reasonable steps to protect Plaintiff'sand the Class Members' PII from disclosure.

Data Breaches Are Avoidable

38. Upon information and belief, the Data Breach was a direct result of Defendant's failure to implement adequate and reasonable data protection procedures, including vendor management, necessary to protect Plaintiff's and

[12] *Ticketmaster Commitments*, https://privacy.ticketmaster.com/our-commitments (accessed June 11, 2024).

Class Members' PII from a foreseeable and preventable risk of unauthorized disclosure.

39. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[13] Ransomware groups frequently implement a double extortion tactic, where the cybercriminal posts portions of the data to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[14]

40. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

Preventative Measures

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans

[13] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).

[14] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

o. Conduct an annual penetration test and vulnerability assessment.

p. Secure your backups.[15]

q. Identify the computers or servers where sensitive personal information is stored.

---

[15] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware- prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

r. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

s. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

t. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

u. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

v. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

w. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.

x. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

y. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

z. To detect network breaches when they occur, consider using an intrusion detection system.

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[16]

41. Defendant's security practices were ineffective since Defendant did not ensure its third-party vendors were responsible for implementing them. When a vendor is using, collecting, or storing personal data, the following are common data protection requirements:

Vendor Management

a. Require the vendor to impose technical and organizational measures to protect personal data, similar to those listed above.

b. Ensure that the vendor requires each individual processing the personal data to be subject to a duty of confidentiality.

c. Require the vendor (and any subcontractors) to comply with all applicable statutes and data protection obligations as the Defendants.

d. Require the vendor to cooperate with reasonable privacy assessments and security audits.

e. Prohibit the vendor from retaining, using, or disclosing personal data for any purpose other than the specified business purpose.

f. Require the vendor to notify the Defendant of a data breach or after vendor makes a determination that it can no longer meet its data protection obligations.

[16] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business- guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

g. Require the vendor to provide timely notice to individuals impacted by a data breach event.

42. Given that Defendant stored the PII of its current and former customers, Defendant could and should have implemented all the above measures to prevent and detect cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class members' PII.

43. Defendant knew and understood unencrypted PII is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding customer PII and of the foreseeable consequences that would occur if Defendant's network (or the network of their vendors) was breached, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

44. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any harms associated with the fraudulent use of their PII.

45. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

46. Personal identifying information is of great value to criminals. Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[17]

47. Given these facts, by transacting business with Plaintiff and Class

[17] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/

Members, collecting and selling their PII, using their PII to market additional products and services to them, and then compromising the privacy of their PII has deprived Plaintiff and Class Members of the benefit of their bargain with Defendants.

48. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an injury in fact. Additionally, the Plaintiff and Class Members are at an increased risk of future harm, including identity theft, fraud, spam, phishing, or other impersonation attacks.

49. There is a substantial risk of future identity theft or fraud where the Plaintiff's and Class Members' PII was targeted by a sophisticated hacker group (ShinyHunters), known for stealing and reselling as much personal and financial data as they can.[18] Furthermore, since 2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (*e.g.*, GitHub, AT&T, Pizza Hut). Upon information and belief, ShinyHunters has accumulated enough personal information from that series of data breaches to be able to open a bank account or commit other fraud using stolen identities.

50. Plaintiff and Class Members face a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a hacker group known for selling personal data on the dark web.

51. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to

---

[18] *What we know about the 'remarkably devious' ShinyHunters hackers allegedly behind the Ticketmaster data leak*, https://www.abc.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928 (accessed June 11, 2024).

mitigate the actual consequences of the Data Breach; (vii) experience an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fail to implement appropriate and reasonable measures to protect the PII.

52. As a result of the Data Breach, unauthorized individuals can easily access the PII of Plaintiff and Class Members. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes.

53. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

54. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[19] With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry

[19] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texaslife-insurance.

unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

55. Since 2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (e.g., GitHub, AT&T, Pizza Hut). The development of "Fullz" packages is highly likely considering the volumes of data acquired by ShinyHunters. In other words, even if certain information such as social security numbers were not included in the PII that was exfiltrated in the Data Breach, criminals can easily create a Fullz package and either sell the information to the highest bidder or use the complete profile to perpetuate fraud or theft.

56. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach and signing up for the credit monitoring and identity theft protection services.

57. Plaintiff's mitigation efforts are also consistent with the several steps that the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[20]

58. PII is a valuable property right. For example, sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[21] In 2019, the data

---

[20] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[21] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

brokering industry was worth roughly $200 billion.[22]

59. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

60. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

61. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

62. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from the Data Breach.

63. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for products or services, customers understood and expected that they were, in part, paying for the protection of their personal data, when in fact,

---

[22] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

Defendant did not provide adequate security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

V. CLASS ALLEGATIONS

64. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

65. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class**
> All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result the April 2, 2024 Data Breach (the "Class").
>
> **Florida Subclass**
> All individuals residing in Florida whose PII was accessed and acquired by an unauthorized party as a result of April 2, 2024 Data Breach (the "Florida Subclass").

66. Collectively, the Class and Florida Subclass are referred to as the "Classes" or "Class Members."

67. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserve the right to amend the definitions of the Classses or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

69. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the

Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendants, upon information and belief, millions of individuals were impacted in Data Breach.

70. Commonality and Predominance: Questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and,

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach

71. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Classes

72. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

73. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff have retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

74. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense

that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

75. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

76. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

77. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

78. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

79. Further, Defendant have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

80. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;

c. Whether Defendant's (or their vendors') security measures to protect their network were reasonable in light of industry best practices;

d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;

f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and

g. Whether adherence to FTC recommendations for protecting personal information would have reasonably prevented the Data Breach

VI. CAUSES OF ACTION

COUNT 1: NEGLIGENCE

(On Behalf of the Plaintiff and the Classes)

81. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

82. Defendant require its customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing ticketing services for live entertainment events.

83. Defendant gathered and stored the PII of Plaintiff and Class Members as part of their business of soliciting its services to their customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

84. Defendant had full knowledge of the types of PII they collect and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

85. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data they obtain.

86. Defendant's duty included a responsibility to ensure its vendors: (i) implemented reasonable measures to detect and prevent unauthorized intrusions into their network; (ii) were contractually obligated to adhere to the requirements of Defendant's privacy policy; (iii) were required to comply with the same statutes and data protection obligations as the Defendants; (iv) were required to submit to regular privacy assessments and security audits; (v) were regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) were obligated to provide timely notice to individuals impacted by a data breach event.

87. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive practices that affect commerce. Deceptive practices, as interpreted and enforced by the FTC, include failing to adhere to a company's own stated privacy policies.

88. Defendant also had a duty to exercise appropriate clearinghouse

practices to remove former customers' PII they were no longer required to retain. Defendant had a duty to promptly and adequately notify Plaintiff and the Classes of the Data Breach.

89. Defendant had a duty to adequately disclose that the PII of Plaintiff and the Classes within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

90. Defendant breached its duties, pursuant to the FTC Act, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former customers' PII it was no longer required to retain;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and,

g. Failing to ensure their vendors implemented data security practices consistent with Defendant's published privacy policies.

91. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that

resulted from the Data Breach was the type of harm the statue was intended to guard against.

92. The injuries resulting to Plaintiff and the Classes because of Defendant failure to use adequate security measures was reasonably foreseeable. Further, the Data Breach was reasonably foreseeable given the Defendant prior experience with cyberattacks and data breaches.

93. Plaintiff and the Class were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of protecting PII transmitted to and maintained on third party systems.

94. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant were in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

95. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

96. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to

further unauthorized disclosures so long as Defendant fail to implement appropriate and reasonable measures to protect the PII.

97. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

98. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

99. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members

COUNT 2: NEGLIGENCE *PER SE*

(On Behalf of the Plaintiff and the Classes)

100. Plaintiff realleges and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

101. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive practices that affect commerce. Deceptive practices, as interpreted and enforced by the FTC, include failing to adhere to a company's own stated privacy policies.

102. Defendant violated Section 5 of the FTC Act by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiff and Class Members information. Defendant further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII.

103. Defendant's violations of Section 5 of the FTC Act, and other state

consumer protection statutes, constitutes negligence *per se.*

104. Plaintiff and Class Members are within the class of persons Section 5 of the FTC Act, and other state consumer protection statutes, were intended to protect. Moreover, the harm that has occurred is the type of harm the FTC Act, and similar state statutes were intended to guard against.

105. But for Defendant wrongful and negligent breach of duties owed to Plaintiff and the Classes, the PII of Plaintiff and the Class would not have been compromised.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fail to implement appropriate and reasonable measures to protect the PII.

107. As a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

108. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake

appropriate and adequate measures to protect the PII in its continued possession.

109. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

110. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT 3: BREACH OF IMPLIED CONTRACT

(On Behalf of the Plaintiff and the Classes)

111. Plaintiff reallege and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

112. Defendant require their customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing ticketing services for live entertainment events.

113. Plaintiff and the Classes entrusted their PII to Defendant. In so doing, Plaintiff and the Classes entered implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and the Classes if their data had been compromised or stolen.

114. Defendant promulgated, adopted, and implemented written privacy policies whereby they promised Plaintiff and Class Members that they would (a) use PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt notice of any unauthorized access and/or theft of their PII, (e) reasonably ensure their vendors safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

115. Plaintiff and Class Members would not have entrusted their PII to

Defendant in the absence of their implied promise to implement reasonable data protection measures.

116. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

117. Defendant breached the implied contracts it made with Plaintiff and the Classes by failing to protect their personal information, by failing to delete the information once the relationship ended, and by failing to provide adequate notice of the Data Breach.

118. As a direct and proximate result of Defendant breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

119. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

120. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT 4: UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Classes)

121. Plaintiff realleges and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

122. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

123. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendants. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit. Defendant sold their PII and used the data to market and sell additional services to Plaintiff and Class Members.

124. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

125. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, they would not have entrusted their PII to Defendants.

126. Plaintiff and Class Members have no adequate remedy at law.

127. Under the circumstances, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon them.

128. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fail to implement appropriate and reasonable measures to protect the PII.

129. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from their wrongful conduct.

/ / /

/ / /

/ / /

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

a) For an Order certifying the Classes, and appointing Plaintiff and her Counsel to represent the Classes;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

c) For injunctive relief and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful acts described herein;

ii. requiring Defendant to protect all data collected during the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete the PII of Plaintiff and Class Members unless Defendant can provide a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII they collect; and

v. requiring Defendant to audit, test, and train their vendors regarding data protection procedures.

d) For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f) For prejudgment interest on all amounts awarded; and

g) Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMANDED

Plaintiff hereby demand a trial by jury on all claims so triable.

Dated: October 11, 2024

Respectfully Submitted,

/s/ Kiley L. Grombacher
Kiley L. Grombacher